PRIVACY IMPACT ASSESSMENT

Consular Launchpad for Enterprise Analytics and Reporting (CLEAR) PIA

1. Contact Information

A/GIS Deputy Assistant Secretary Bureau of Administration Global Information Services

2. System Information

(a) Name of system: Consular Launchpad for Enterprise Analytics and Reporting

(b) Bureau: Consular Affairs

(c) System acronym: CLEAR

(d) iMatrix Asset ID Number: 6126

(e) Reason for performing PIA: Click here to enter text.

☐ New system

☐ Significant modification to an existing system

☒ To update existing PIA for a triennial security reauthorization

(f) Explanation of modification (if applicable): In addition to the update for the security reauthorization, the Consular Affairs Business Intelligence (CABI) portal has been renamed as the Consular Launchpad for Enterprise Analytics and Reporting (CLEAR) portal.

3. General Information

(a) Does the system have a completed and submitted Security Categorization Form (SCF)?

☒Yes

☐No - Contact IRM/IA at IASolutionCenter@state.gov for assistance.

(b) What is the security Assessment and Authorization (A&A) status of the system?

The CLEAR portal, (formally the Consular Affairs Business Intelligence (CABI)) Authority to Operate expires February 29, 2020. The authorization is valid until rescinded or the expiry date of February 29, 2020.

(c) Describe the purpose of the system:

The purpose of the CLEAR portal is to provide a centralized interface for Consular Affairs dashboards, reports, and ad-hoc reporting and analysis tools. The CLEAR portal is the primary implementation tool of the Consular Affairs Business Intelligence Center of Excellence (CA BI COE). It provides the framework and service to CA users to access

consular data extracted from other CA sources through the Consular Consolidated Database (CCD). The CLEAR portal pulls data from the CCD, which has data that originated from the following CA systems: Non-Immigrant Visa (NIV), Immigrant Visa Overseas (IVO), Consular Electronic Application Center (CEAC), American Citizen Services (ACS) suite of systems, and the Travel Document Issuance System (TDIS). The extracted data is then aggregated and loaded into database structures optimized for reporting (also referred to as the CA Enterprise Data Warehouse and data marts) or loaded into the SAP High-performance analytic appliance (HANA) database.

(d) Describe the personally identifiable information (PII) that the system collects, uses, maintains, or disseminates:

- Names of individuals
- Business contact information
- Personal phone numbers
- Personal email addresses
- Personal addresses
- Place of birth
- Date of birth
- Mother's maiden name
- Social Security Number
- Social media accounts of individuals
- Government Issued IDs (e.g., passport numbers or national identification numbers of visa applicants)

(e) What are the specific legal authorities and/or agreements that allow the information to be collected?

- 22 U.S.C. § 3927 (Chief of Mission)
- 8 U.S.C. 1101-1105a; 1151-1363a;1401-1504 & 1151-1363a03 (The Immigration and Nationality Act of 1952, as amended)
- 18 U.S.C. 911, 1001, 1541-1546 (Crimes and Criminal Procedure);
- 22 U.S.C. 211a-218, (Passports)
- 22 U.S.C. 2651a (Organization of Department of State)
- Executive Order 11295, August 5, 1966, 31 FR 10603; (Authority of the Secretary of State in granting and issuing U.S. passports)
- 22 C.F.R. Parts 50 and 51 (Nationality Procedures and Passports)
- 26 U.S.C. 6039E (Information Concerning Residence Status)
- 22 C.F.R. Parts 40-42, and 46 (Visas)

(f) Is the information searchable by a personal identifier (e.g., name or Social Security

number)?

☒Yes, provide:

- SORN Name and Number:
  STATE-26 - Passport Records, March 24, 2015
  STATE-05 - Overseas Citizens Records and Other Overseas Records, September 8, 2016
  STATE-39 Visa Records, June 15, 2018

☐No, explain how the information is retrieved without a personal identifier.

(g) Does the existing SORN need to be amended to reflect the inclusion of this new or significantly modified system? ☐Yes ☒No

If yes, please notify the Privacy Division at Privacy@state.gov.

(h) Is there a records retention schedule submitted to or approved by the National Archives and Records Administration (NARA) for this system? ☒Yes ☐No

(If uncertain about this question, please contact the Department's Records Officer at records@state.gov .)

If yes provide:
Schedule number, Length of time the information is retained in the system, and Type of information retained in the system:

B-09-002-02b Intermediary Records
Description: Immigrant Visa, Non-immigrant Visa, and Consular Consolidated Database hard copy and electronic input records, including applications, supplemental questionnaires, refusal worksheets and supporting or related documentation and correspondence, relating to persons who have been refused immigrant or nonimmigrant visas (including quasi-refusals), under the following section(s) of law: INA subsections 212(a)(1)(A)(i), (iii), and (iv); (2); (3); (6)(c), (E), and (F); (8); (9)(A) (if alien convicted of an aggravated felony), and (C); and 10(D) and (E); 222(g); Title IV of the Helms-Burton Act (22 USC 6021 et seq.); any cases requiring the Department's opinion code00 (Except quasi-refusal cases under (6)(C)(i)); INA subsection 212(a)(10)(C); Quasi-Refusals under 212(a)(6)(C)(i); 212(a)(9)(B); INA subsection 212(f); and Section 5(a)(1) of the Tom Lantos Block Burmese JADE (Junta's Anti-Democratic Efforts) Act of 2008.

Also includes output records such as adhoc and other reports that contain summarized or aggregated information created by combining data elements or individual observations from a single master file or database.

Disposition: Temporary. Destroy upon verification of successful creation of the final document or file, or when no longer needed for business use, whichever is later.

DispAuthNo: DAA-GRS-2017-0003-0002

4. Characterization of the Information

(a) What entities below are the original sources of the information in the system? Please check all that apply.

☒ Members of the Public

☒ U.S. Government employees/Contractor employees (DoS business information to assigned privileges to access Passport systems to perform specified tasks).

☒ Other (people who are not U.S. Citizens or LPRs)

(b) If the system contains Social Security Numbers (SSNs), is the collection necessary?

☒Yes ☐No

- If yes, under what authorization?

26 U.S.C. 6039E (Information Concerning Resident Status);
Executive Order 9397, November 22, 1943 and Executive Order 13478, November 18, 2008 (amending E.O. 9397)

(c) How is the information collected?

The information for the CLEAR portal reports are collected directly (database to database) from the CCD which houses information from consular systems, all of which reside outside the CLEAR portal system boundary. CLEAR is merely a centralized interface for various systems within the Bureau of Consular Affairs.

(d) Where is the information housed?

☒ Department-owned equipment

☐ FEDRAMP-certified cloud

☐ Other Federal agency equipment or cloud

☐ Other

- If you did not select "Department-owned equipment," please specify.

(e) What process is used to determine if the information is accurate?

The CCD information comes directly from foreign individuals who are applying for visas, US citizens applying for passports, and information entered by consular officers into the source systems. The CLEAR portal only pulls data from source systems (IVO, CEAC, NIV, ACS and TDIS) via the CCD and therefore relies on the source systems to maintain and supply accurate data.

(f) Is the information current? If so, what steps or procedures are taken to ensure it remains current?

Information from the CCD is current and is pulled into the CLEAR portal databases at least once a week.

(g) Does the system use information from commercial sources? Is the information publicly available?

No, the CLEAR system does not acquire information from commercial sources nor is the information it gathers publicly available.

(h) Is notice provided to the individual prior to the collection of his or her information?

The CLEAR portal gets its data from other CA information systems addressed in paragraph 3(c). CLEAR does not collect any data directly from any individual. Individuals are provided notice when they provide their information to the various systems that CLEAR is pulling the information from.

(i) Do individuals have the opportunity to decline to provide the information or to consent to particular uses of the information? ☐Yes ☒No

- If yes, how do individuals grant consent?

- If no, why are individuals not allowed to provide consent?

The CLEAR portal gets its data from other CA information systems addressed in paragraph 3(c). CLEAR does not collect any data directly from any individual. Should individuals want to decline to provide their information, they would need to do so at the original point of collection for the source systems.

(j) How did privacy concerns influence the determination of what information would be collected by the system?

CLEAR does not collect information from the public. CLEAR receives information from CA systems listed in paragraph 3(c). CLEAR merely acts as a centralized interface for various systems within the Bureau of Consular Affairs. However, concerns include unauthorized access, disclosure, modification, and/or misuse of the data by users and/or a security breach. These risks were considered during the system design and security configuration. The PII collected by CLEAR is the minimum necessary to perform the actions required by this system to provide a centralized interface for dashboards, reports, and ad hoc reporting and analysis tools for CA users.

5. Use of information

(a) What is/are the intended use(s) for the information?

The information is used to generate reports and compile metrics related to consular operations and transactions, such as visa and passport applications and applicants, so that consular professionals can perform various types of analyses, including fraud detection, resource allocation, and determination of the cost of services.

(b) Is the use of the information relevant to the purpose for which the system was designed or for which it is being designed?

Yes. The PII is used in the management of the visa and passport operations by CA personnel to compile metrics related to consular operations and transactions for decision making purposes.

(c) Does the system analyze the information stored in it? ☒Yes ☐No

If yes:

(1) What types of methods are used to analyze the information?

The reports from the CLEAR portal display metrics based on a category, comparisons based on trends and averages, and bring together data from different systems to show relationships of the data.

(2) Does the analysis result in new information? Yes.

(3) Will the new information be placed in the individual's record? ☐Yes ☒No

(4) With the new information, will the Department be able to make new determinations about the individual that would not have been possible without it? ☒Yes ☐No

6. Sharing of Information

(a) With whom will the information be shared internally and/or externally? Please identify the recipients of the information.

The main internal stakeholders are within Consular Affairs, with other Department of State bureaus such as Diplomatic Security (DS) and the Bureau of Population, Refugees, and Migration (PRM) occasionally requesting reports from the CLEAR system. No one outside of the Department of State has access to the CLEAR portal itself or the data within the underlying data warehouse.

(b) What information will be shared?
All of the PII mentioned in 3(d) will be shared through dashboards, reports, ad hoc reporting tools, and analysis tools.

(c) What is the purpose for sharing the information?

Information is shared for the purpose of decision support, operational improvement, workload assessment and forecasting, resource planning, and fraud analysis and investigation reports for use by Consular Affairs. DS and PRM use reports for fraud analysis and investigations in support of their missions.

(d) The information to be shared is transmitted or disclosed by what methods?
After the CLEAR portal manipulates the data and produces an electronic report or file, the authorized user can then save it on a local or network drive, or send it as an email attachment. The report can also be printed or faxed.

(e) What safeguards are in place for each internal or external sharing arrangement?
Supervisors along with information system security officers (ISSOs) determine the access level depending on job function and level of clearance.

Information is shared by secure transmission methods permitted by internal Department of State policy for the handling and transmission of Sensitive but Unclassified (SBU) information. Access to electronic files is protected by inherited security controls from the Department of State domain infrastructure. All accounts are under the supervision of system managers. Audit trails track and monitor usage and access. Defense in depth is deployed as well as roles assigned based on least privilege. Finally, regularly administered security and privacy training informs authorized users of proper handling procedures.

(f) What privacy concerns were identified regarding the sharing of the information? How were these concerns addressed?

Privacy concerns regarding the sharing of information focus on two primary sources of risk:

1) Accidental disclosure of information to non-authorized parties:

Accidental disclosure is usually due to inadequate document control (hard copy or electronic), inadequate PII and security training, or insufficient knowledge of roles, authorization and need to know policies. In addition, social engineering, phishing, and firewall breaches can also represent a risk of accidental disclosure of information.

2) Deliberate disclosure/theft or information to non-authorized parties regardless of motive whether monetary, personal or other.

These risks are mitigated using a multi-faceted approach to security:

1) Frequent security training for all personnel regarding information security, including the safe handling and storage of PII, Sensitive but Unclassified, and all higher levels of classification, and signing a user agreement.

2) Strict role based access control, based on approved roles and responsibilities, authorization, need- to-know, and clearance level.

3) Implementation of management, operational, and technical controls regarding separation of duties, least privilege, auditing, and personnel account management.

7. Redress and Notification

(a) What procedures allow individuals to gain access to their information?

The CLEAR portal does not collect information directly from individuals nor do individuals have access to the CLEAR data. CLEAR acquires information from CCD to perform functions.

An individual would need to follow procedures outlined for the source system where they provided information, i.e., the CCD, to gain access to their information.

Individuals may also visit the Department of State public site and/or the Department of State Privacy Act/FOIA website for the privacy policy which includes procedures on how to obtain access to records by contacting the listed offices by phone or by mail.

(b) Are procedures in place to allow an individual to correct inaccurate or erroneous information?

☐Yes ☒No

If yes, explain the procedures.

If no, explain why not.

CLEAR does not collect information directly from the public. The information is acquired from other CA systems listed in paragraph 3(c). Data is copied from the original source systems in a one-way pull from the source systems into the CLEAR data warehouse. Individuals must follow processes of the source systems used to apply for the specific service to request correction of information. Notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals can also follow procedures outlined in SORNs STATE-26, STATE-05, and STATE 39, listed in paragraph 3(f) as above that are posted on the Department of State's Privacy website at www.state.gov/privacy.

(c) By what means are individuals notified of the procedures to correct their information?
CLEAR does not collect information from the public. The information is acquired from other CA systems listed in paragraph 3(c). Individuals must follow processes of the source systems used to apply for the specific service to request correction of information. Notice to correct personal information is provided at the source site where applicants apply for specific services.

Individuals can also follow procedures outlined in SORNs STATE-26, STATE-05 and STATE 39 addressed in paragraph 3(f) that are posted on the Department of State's Privacy website at www.state.gov/privacy.

8. Security Controls

(a) How is the information in the system secured?

Information in the CLEAR portal is secured where risk factors are mitigated through the use of defense in depth layers of security, including management, operational and technical security controls, auditing, firewalls, physical security, and continuous monitoring. Internal access is limited to authorized Department of State users, including cleared contractors who have a justified need for the information in order to perform official duties.

CLEAR personnel access accounts are created and assigned the appropriate level of privileges approved by the supervisor. The user can then perform the tasks associated with the privileges authorized. Additionally, CLEAR generates audit records that display time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked for record searches. This information is used to track Department of State user activity for auditing. Audit Trail Reports can be run to show reports that were executed/ accessed by users at any time. Screen shots depict access for a specific date/time to a file, along with the list of users and their transactions.

CLEAR is configured according to State Department Security Configuration Guides to optimize security while still providing functionality. Applicable National Institute of Standards and Technology (NIST) 800-53 and privacy overlays of management, operational, and technical controls are in place and are tested as part of the continuous monitoring program. Vulnerabilities noted during the testing of the system are reported appropriately and are tracked until compliant or acceptably mitigated.

(b) Describe the procedures established to limit access to only those individuals who have an "official" need to access the information in their work capacity.

Internal access to the CLEAR portal is limited to authorized Department of State users, including cleared contractors, who have a justified need for the information in order to perform official duties, and to auditors with the Office of Inspector General (OIG). Authorized usuers with an official need to access is determined by the users supervisor.

Access to information within the CLEAR portal is role based and controlled by Business Objects security groups. Each report within the CLEAR portal is assigned to a Business Objects security group. Each security group is also associated with either an Active Directory group or role in an external system. For a user to access a report, they must be part of the specific Active Directory (AD) group or have the external role associated with the Business Objects security group. The AD groups and external roles associated with the report are determined by the Business Units.

Access to the information in the system is role based, and restricted according to approved job responsibilities and requires managerial concurrence. Access control lists permit categories of information and reports to be restricted. Information System Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) What monitoring, recording, and auditing safeguards are in place to prevent the misuse of the information?

Various technical controls are in place to deter, detect, and defend against the misuse of personally identifiable information (PII). Any changes (authorized or not) that occur to data are recorded. In accordance with Department of State Security Configuration Guides, auditing is also enabled for this specific system to track the following events on the host operating systems, and back-end database servers:

- Multiple logon failures;
- Logons after hours or at unusual times;
- Failed attempts to execute programs or access files;
- Addition, deletion, or modification of user or program access privileges; or
- Changes in file access restrictions.

The purpose of the CLEAR audit trail is to document unintended modification or unauthorized access to the system and to dynamically audit retrieval access to designated critical data. If an issue were to arise, administrators of the system would review (audit) the logs that were collected from the time a user logged on until the time he/she signed off. This multilayered approach to security controls greatly reduces the risk that PII will be misused.

(d) Explain the privacy training provided to the authorized users of the system.

In accordance with Department of State computer security policies, all users are required to complete the annual mandatory PS800 Cyber Security Awareness training and the one-time privacy (PA459 Protecting Personally Identifiable Information) training. In order to retain access, each user must annually complete the Cyber Security Awareness Training, which has a privacy component. Additionally, upon accessing the CLEAR portal, all users are presented with a Privacy Agreement.

In order to access the actual reports, the user must acknowledge that they have read the Privacy Agreement.

(e) Are any security controls, such as encryption, strong authentication procedures, or other controls, in place to make the information unusable to unauthorized users?

☒Yes ☐No

If yes, please explain.

Routine monitoring, testing, and evaluation of security controls are conducted to ensure the safeguards continue to function as desired. Many of the security controls implemented to make information unusable or inaccessible to unauthorized users include access enforcement, separation of duties, least privilege, audit review, analysis, and reporting, identification and authentication of organizational users, information system monitoring and numerous media controls.

The Information Integrity Branch (IIB) provides administrative life-cycle security protection for the Department of State's information technology systems and information resources. All systems must comply with all guidelines published by Systems Integrity Division, in addition to all Security Configuration Guides published by Diplomatic Security. Adherence to these guides is verified during the system's Assessment and Authorization process.

The CLEAR uses Transmission Control Protocol/Internet Protocol (TCP/IP) for data transport across the network. Data in transit is encrypted. The TCP/IP suite consists of multiple layers of protocols that help ensure the integrity of data transmission, including handshaking, header checks, and re-sending of data if necessary.

(f) How were the security measures above influenced by the type of information collected?

The information in CLEAR contains PII of U.S. citizens, legal permanent Residents (LPRs) and foreigners. Due to the sensitivity of information collected, information is secured by effective procedures for access authorization, account housekeeping, monitoring, recording, and auditing.

Organizations or individuals whose PII is breached or exposed to unauthorized users could face inconvenience, distress, damage to standing or reputation, threats to personal safety, and financial loss. Security measures are in place to minimize these risks, and to minimize the risk of harm to State Department programs or the public interest through an unauthorized release of sensitive information. The security measures listed above in paragraph 8(e) are implemented to secure the data in the system in compliance with federal laws and policies, including Department policies.

9. Data Access

(a) Who has access to data in the system?

The following personnel have access to these systems:

The CLEAR portal may be accessed by authorized users within the Department of State. The reports and data that a user can see when accessing the CLEAR portal depends on the permissions that have been granted to that user.

There are four types of user roles: System Administrator, Database Administrator, Application Security Manager and users.

System Administrator: System administrative staff maintain the system and user accounts, perform system backups, control access control lists, manage the operating system changes and other actions to keep CLEAR operational. They have the same security responsibilities of users, but their responsibilities are expanded to recognize their privileged user status. Systems administrators restrict themselves from using their position to turn off/destroy audit trails, giving unauthorized individuals privileged access, and modifying the system to negate automated security mechanisms.

Database Administrator: The Database Administrator performs maintenance, troubleshoots technical issues, installs software and patches, and other actions needed to keep the system operational.

Application Security Manager: Security Managers administer and monitor the activities to protect the system. The Application Security Manager utilizes the Central Management Console to manage user access levels. The Application Security Manager, responsible for granting users access to application specific data via reports and dashboards, employs the need to know policy to enforce the most restrictive set of rights/privileges needed by users to perform their job.

CA Users - Access to CLEAR is restricted to cleared Department of State direct hire and contractor employees. The CLEAR users are assigned access privileges based on their job functions. All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties. **Users:** Authorized individuals who acquire

information from CLEAR to perform duties using generated reports dashboards, ad hoc reporting tools, and analysis tools.

All access permissions are enforced by Business Objects groups according to the principle of least privilege and the concept of separation of duties. Business Objects groups are populated by linking them to an external authoritative source (Active Directory group or external application role).

(b) How is access to data in the system determined?
User access to information is restricted according to job responsibilities and requires managerial level approvals. Access control lists permit categories of information and reports that are to be restricted. Information System Security Officers determine the access level needed by a user (including managers) to ensure it correlates to the user's particular job function and level of clearance.

(c) Are procedures, controls or responsibilities regarding access to data in the system documented? ☒Yes ☐No
Procedures and controls are documented in the System Security Plan. The Plan includes information and procedures regarding access to data in the CLEAR portal.

(d) Will all users have access to all data in the system, or will user access be restricted? Please explain.

No, all users will not have access to all data in the system. The CLEAR portal has a very restrictive policy regarding accessing sensitive data. There is a process is in place whereby each Business Unit must define requirements and authorize users for all reports from CLEAR for which they are the data owners.

There are four types of user roles, each with restricted access to specific information and areas of the system: System Administrator, Database Administrator, Application Security Manager and users (See 9(a) above). The System Administrator, Database administrator, and the Application Security Manager can see and access the data in the system. The users can only view information and generate reports that they have been given permission to run. They cannot change information in CLEAR.

All access is enforced by user profiles according to the principle of least privilege and the concept of separation of duties.

(e) What controls are in place to prevent the misuse (e.g. unauthorized browsing) of data by users having access to the data? The CLEAR system information is protected by multiple layers of security controls including:

- Access control policies and access enforcement mechanisms control access to PII.

- Separation of duties is implemented; access is role based as required by Department of State policy.

- CLEAR System and Database Administrators, the Application Security Manager and internal users must use dual factor authentication utilizing Personal Identification Verification/Common Access Card (PIV/CAC) and Personal Identification Number (PIN) to access data. Users are uniquely identified and authenticated before accessing PII and while logged in can be traced to their actions performed.

- Least Privileges are restrictive rights/privileges or access of users for the performance of specified tasks. The Department of State ensures that users who must access records containing PII only have access to the minimum amount of PII, along with only those privileges (e.g., read, write, execute) that are necessary to perform their job duties.

- System and information integrity auditing are implemented to monitor and record unauthorized access/use of information.